

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks



CYBERSECURITY

[Navy Investigating Whether Ship Collision Resulted from Cyber-Attack](#)

The United States Navy is investigating whether the recent collision of the USS John S. McCain with a Liberian tanker off Singapore may have been caused by a cyber-attack. According to Admiral John Richardson, the investigation will look into “the possibility of cyber intrusion or sabotage.” [Read more](#)

[NIST Updates Digital Identity Guidelines for Federal Agencies](#)

This month, the National Institute of Standards and Technology (NIST) announced in a bulletin that it has updated its Digital Identity Guidelines, which “provides agencies with technical guidelines regarding the digital authentication of users to federal networked systems.” The bulletin outlines the components of digital identity—identity proofing, authentication, and federation for federal agencies to use to protect the identities of their employees. [Read more](#)

INTERNATIONAL DATA PRIVACY

[Five Focus Areas in Preparation for GDPR Compliance](#)

In less than 300 days, the European General Data Protection Regulation (GDPR) will go into effect and forever change the privacy landscape. Leading industry organization Gartner, Inc., predicts that more than 50 percent of companies affected by the GDPR will not be fully compliant. Of course, the affected companies will include both European and non-European companies. Bart Willemsen, research director at Gartner, says, “Threats of hefty fines, as well as the increasingly empowered position of individual data subjects tilt business case for compliance and should cause decision makers to re-evaluate measures to safely process personal data.” [Read more](#)

August 31, 2017

FEATURED AUTHORS:

[Linn Foster Freedman](#)
[Benjamin C. Jensen](#)
[James Merrifield](#)
[Kathryn M. Rattigan](#)

FEATURED TOPICS:

[Cybersecurity](#)
[Data Breach](#)
[International Data Privacy](#)
[Drones](#)
[Privacy Tip](#)
[Virtual Currency](#)

VISIT + SHARE:

[Insider Blog](#)
[R+C website](#)
[Twitter](#)
[Facebook](#)
[LinkedIn](#)

DATA BREACH

[Delaware Updates Its Data Breach Notification Law](#)

A total of 48 states have enacted data breach notification laws, and they frequently are amended and updated. The most recent state to update its law is Delaware.

A significant change in the new law is that Delaware residents who are affected by a data breach of their personal information must be offered 12 months of free credit monitoring. In addition, those affected by a breach must be notified of the incident as soon as possible but no later than 60 days after the discovery of the breach. [Read more](#)

VIRTUAL CURRENCY

[Alabama Adopts New Law Governing Virtual Currency Transactions](#)

This month, a new law governing virtual currency and online transactions went into effect in Alabama. The Alabama Monetary Transmission Act was passed by the legislature in May and replaces the Sale of Checks Act, which had been in effect since 1961. The legislation regulates transactions involving virtual currency, such as BitCoin, as well as traditional money transfers.

Under the Act, unless exempted by the statute, persons engaged in the business of monetary transmissions must obtain a license from the commission. Among the persons and entities excluded from the act and its licensing requirements are banks, bank holding companies, futures merchants, governmental entities, broker-dealers, and securities clearing firms. [Read more](#)

DRONES

[Drones Delivering Medical Supplies in East Africa but not in U.S.](#)

Residents in remote areas of Tanzania and Rwanda in East Africa are receiving medical supplies through the use of drones, far surpassing similar efforts in the U.S., according to Robert Graboyes, a senior research fellow at George Mason University. In Rwanda alone, according to RealClear Health, drones have delivered 2,600 units of blood and have traveled more than 62,000 miles to do so.

Despite the fact that many residents in remote areas in the U.S. could benefit from the delivery of medical supplies through the use of drones, Graboyes says that the U.S. is lagging behind other countries, including East Africa, because of strict Federal Aviation

Administration rules around the use of drones. [Read more](#)

PRIVACY TIP #103

Smartphone Replacement Parts Subject to Hacking

You drop your smartphone and now there are a million cracks and you can hardly read your texts. Getting the screen replaced by the manufacturer of the phone is usually expensive, and sometimes it is so expensive that it makes more sense just to buy a new phone.

But some will bypass the manufacturer and buy a replacement screen from a third-party to save money. Think twice about going this route.

According to a study led by researchers at Ben Gurion University, “Shattered Trust: When replacement smartphone components attack,” certain replacement parts for smartphones that are bought from third-party manufacturers, including replacement displays, NFC readers, and components for wireless charging, can be used to hack into the smartphone.

The researchers found that third-party source code can be integrated into the vendor’s source code, and the screen actually looks like the regular screen but is accessing all of the information on the phone in the background.

This occurs when a malicious chip is put into the screen, which can then can record all communication of the smartphone, including emails, text messages, keystrokes for telephone calls, and using the device for illegal activity using apps.

The components are so sophisticated that they look like the real component, and technicians might not be able to tell the difference. Even more concerning is the fact that antivirus tools don’t detect it, and integrity checks and security protocols are not available for third-party component parts.

So, although the smartphone manufacturers charge a lot for component parts, consider using the manufacturer’s component parts instead of buying a cheaper one online from a third-party manufacturer. In this case, you do get what you pay for—a compromise of all of the information on your smartphone.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | [rc.com](#)

Robinson & Cole LLP



be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.